Lampi di Cassandra/ I falsi certificati di Tor

(236) —Il sistema dei certificati SSL largamente utilizzati in Rete ha debolezze intrinseche, lo dimostra l'attacco portato alla rete…

Lampi di Cassandra/ I falsi certificati di Tor

Figure 1:

(236)—Il sistema dei certificati SSL largamente utilizzati in Rete ha debolezze intrinseche, lo dimostra l'attacco portato alla rete Tor tramite la violazione della certificate authority DigiNotar.

5 settembre 2011—La notizia di questa violazione informatica subita dall'autorità di certificazione DigiNotar emersa e molto commentata la scorsa settimana ha avuto una certa risonanza perché alcuni dei certificati compromessi riguardavano server di Google.

Molti abitanti della Rete hanno probabilmente solo gettato un'occhiata distratta alla notizia, e quelli che l'hanno letta non vi hanno probabilmente trovato specifici motivi per un approfondimento.

Madornale errore!

E' invece importante sotto diversi punti di vista, anche come esempio didattico per capire luci ed ombre del modello di fiducia dei certificati SSL. Partiamo innanzitutto da questo aspetto.

Nel modello di autenticazione e fiducia ormai standard, basato su autorità di certificazione completamente indipendenti tra loro, è sufficiente la violazione di una sola di esse per compromettere, almeno fino alla scoperta del fatto, tutto il modello.

La catena di fiducia è resistente solo quanto l'anello più debole, e la compromissione di un'unica autorità di certificazione permette di portare attacchi mirati di tipo MITM (Man In The

Middle—uomo nel mezzo) come quello potenzialmente subito dalla rete Tor e riassunto in questo lungo e dettagliato messaggio di Roger Dingledine.

Ma cosa è successo in termini pratici? Chi ha violato la (piccola) autorità di certificazione DigiNotar, ha usato le informazioni (chiavi) rubate per creare certificati a nome di diverse organizzazioni. Oltre a Google sono stati anche creati dei certificati per il dominio **.torproject.org*.

Questi certificati non sono tecnicamente falsi, sono tecnicamente autentici, e tutti i browser del mondo li riconosceranno come appartenenti a *torproject.org*, perché tutti i browser del mondo, nell'attuale modello di fiducia, contengono i certificati di tutte le autorità di certificazione commerciali, e quindi considerano validi i certificati da esse emessi.

In pratica esistono i certificati autentici di *torproject.org*, certificati da un'altra autorità di certificazione, e quelli "falsificati".

Poiché i certificati di tutte le autorità di certificazione si trovano già memorizzati in tutti i browser (incluso ovviamente quello di DigiNotar), ambedue i certificati di *torproject.org*, quello autentico e quello di DigiNotar, vengono accettati senza segnalazioni all'utente.

Questo ha reso possibile reindirizzare gli utenti che volevano collegarsi a *torproject.org* verso falsi siti dotati del certificato falsificato che sarebbe stato riconosciuto come autentico. E' quindi teoricamente possibile che siano stati ad esempio scaricate copie di Tor, di bundle Tor di altre applicazioni distribuite per mezzo del sito *torproject.org*.

E' appena il caso di notare che l'aggressore ha realizzato anche altri certificati per portare attacchi informatici, come quelli, impossibili ma superpotenti, per **.com* e **.org*; maggiori particolari in questo ulteriore post.

Ed adesso le buone notizie.Non esistono ad oggi evidenze che attacchi di questo tipo siano stati effettivamente condotti contro Tor.Tramite il certificato contraffatto non sono possibili attacchi che minino il funzionamento della rete Tor nel suo complesso, ma "solo" singoli utenti.

Coloro che ritenessero di poter essere stati vittime di un tale attacco avendo scaricato software da *torproject.org*, possono semplicemente scaricarne e reinstallarne una nuova copia, dopo aver controllato che il certificato del sito a cui sono connessi sia stato emesso da DigiCert Inc., e non da DigiNotar.

Per maggiore sicurezza è possibile disabilitare o cancellare il certificato root di DigiNotar dal browser: potrà comunque essere riabilitato per utilizzare un sito che dotato di un certificato autentico di DigiNotar.

Infine c'è una piccola possibilità che questo clamoroso evento possa contribuire ad un ripensamento del modello di fiducia che la Rete ha con troppa superficialità adottato.

Per finire suggerisco un semplice e sempre utile esercizio di paranoia: "Perché gli ignoti autori dell'intrusione hanno creato un certificato fasullo di torproject.org, e non piuttosto quelli di tutte le principali banche europee?"

Lo svolgimento dell'esercizio viene però lasciato alla diligenza del lettore.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"

Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.